AMENDMENTS TO THE CLAIMS:

1. (Original) In a computer network arrangement comprising a home network having at least one home network server and a firewall for protecting said home network server, a relay server outside of said home network, and a client having a permanent IP address within said home network, a method for maintaining secure communications between the home network server and the client when said client roams outside of said home network to a new location, said method comprising:

establishing a new IP address for the new client location;

sending a registration message to said relay server identifying said new IP address location;

authenticating said registration message;

encapsulating and transmitting said registration message to said home server;

registering said new IP address as a care-of-address for said client at said home server;

confirming the registration of said new IP address with said client;

establishing a security association between said home server and said relay server on behalf of said client;

performing network address translation between the client's permanent IP address and the client's new IP address;

tunneling packets addressed for said client between said home server and said relay server based on the established security association and said address translation for said client; and

decapsulating said packets at said relay server and forwarding said packets to said client.

2. (Original) The method of claim 1, wherein said home network further comprises a multiplexer subsystem.

3. (Original) The method of claim 1, wherein at least a portion of the communications from said client to said home server are in HTTP Request-format.

4. (Original) The method of claim 3, wherein at least a portion of the communications from said home server to said client are in HTTP Response-format.

5. (Original) The method of claim 4, wherein at least a portion of the communications from said client to said home server are encapsulated in UDP packets.

6. (Original) The method of claim 5, wherein at least a portion of the communications from said home server to said client are encapsulated in UDP packets.

7. (Original) The method of claim 1, wherein said method further comprises the step of: providing a network gateway, wherein said network gateway operates to tunnel packets through said firewall to said home server.

8. (Original) The method of claim 7, wherein said network gateway is a Virtual Private Network gateway.

9. (Original) In a computer network arrangement comprising a home network having at least one home network server and a firewall for protecting said home network server, a relay server outside of said home network, and a client having a permanent IP address within said home network, a method for maintaining secure communications between the home network server and the client when said client roams outside of said home network to a new location, said method comprising:

establishing a new IP address for the new client location;

sending a registration message to said home server identifying said new IP address location;

encapsulating and transmitting said registration message to said home server;

registering said new IP address as a care-of-address for said client at said home server;

confirming the registration of said new IP address with said client;

establishing a security association between said home server and said client;

performing network address translation between the client's permanent IP address and the client's new IP address; and

tunneling packets addressed for said client between said home server and said client based on the established security association and said address translation for said client.

10. (Original) The method of claim 9, wherein said home network further comprises a multiplexer subsystem.

11. (Original) The method of claim 9, wherein at least a portion of the communications from said client to said home server are in HTTP Request-format.

12. (Original) The method of claim 11, wherein at least a portion of the communications from said home server to said client are in HTTP Response-format.

13. (Original) The method of claim 12, wherein at least a portion of the communications from said client to said home server are encapsulated in UDP packets by said multiplexer subsystem.

14. (Original) The method of claim 13, wherein at least a portion of the communications from said home server to said client are encapsulated in UDP packets by said multiplexer subsystem.

15. (Original) The method of claim 9, wherein said method further comprises the step of: providing a network gateway, wherein said network gateway operates to tunnel packets through said firewall to said home server.

16. (Original) The method of claim 15, wherein said network gateway is a Virtual Private Network gateway.

17 - 18. (Canceled)

19. (Original) The method of claim 1, wherein, said method further comprises the steps of:

generating a first message in HTTP Request-format,

transmitting said first message in HTTP Request-format through said firewall;

processing said first message, wherein said first message is encapsulated in UDP packets and forwarded to its intended recipient;

generating a second message in response to said first message, wherein said second message is encapsulated in UDP packets;

translating said second message into HTTP Response-Format; and

transmitting said second message to its intended recipient.

20. (Original) The method of claim 9, wherein, said method further comprises the steps of:

generating a first message in HTTP Request-format,

transmitting said first message in HTTP Request-format through said firewall;

processing said first message, wherein said first message is encapsulated in UDP packets and forwarded to its intended recipient;

generating a second message in response to said first message, wherein said second message is encapsulated in UDP packets;

translating said second message into HTTP Response-Format; and

transmitting said second message to its intended recipient.

21. (New) A method of establishing and maintaining secure communications between a home network server that is associated with a home network and a client when the client roams from the home network to a new location outside of the home network, the method comprising:

at the client, establishing a new Internet Protocol address associated with the new location, wherein the client has a permanent Internet Protocol address associated with the home network;

at the client, transmitting a registration message, to a relay server that is coupled to the home network server, wherein the registration message identifies the new Internet Protocol address associated with the permanent Internet Protocol address;

at the relay server, authenticating the registration message;

at the relay server, encapsulating the registration message;

at the relay server, transmitting the encapsulated registration message to the home network server;

establishing a security association between the home network server and the relay server;

at the home network server, registering the new Internet Protocol address as a care-of-address for the client;

at the home network server, transmitting a reply message to the client confirming registration of the new Internet Protocol address as the care-of address for the client, thereby establishing a tunnel between the home network server and the client via the relay;

establishing a security association between the home network server and the client inside the tunnel;

at the home network server, performing network address translation between the permanent IP address and the new Internet Protocol address for packets addressed to the client; and

at the home network server, encapsulating the packets that are addressed to the client based on the security association between the home network server and the client.

22. (New) The method of claim 21, wherein the home network comprises a firewall proxy.

23. (New) The method of claim 21, further comprising:

for traffic between the client and the home network server, tunneling the encapsulated packets is based on the security association between the home network server and the client.

24. (New) The method of claim 23, wherein establishing the security association between the home network server and the client comprises:

at the client, authenticating the home network server;

at the home network server, authenticating the client;

establishing a secure channel for negotiations between the client and the home network server; and

using the secure channel, negotiating security parameters to establish the security association between the client and the home network server, wherein the security parameters comprise an encryption method, an integrity method, and a lifetime of the security association.

25. (New) The method of claim 23, wherein the tunneling of the encapsulated packets comprises:

for outbound traffic, at the relay server, decapsulating the encapsulated packets;

at the relay server, encapsulating the decapsulated packets using the client's new Internet Protocol address; and

at the relay server, transmitting the encapsulated decapsulated packets to the client; and

for inbound traffic, at the relay server, decapsulating the encapsulated packets;

at the relay server, encapsulating the decapsulated packets using the home network server Internet Protocol address; and

at the relay server, transmitting the encapsulated decapsulated packets to the home network server.

26. (New) The method of claim 21, wherein establishing the security association between the home network server and the relay server comprises:

at the relay server, authenticating the home network server;

at the home network server, authenticating the relay server;

establishing a secure channel for negotiations between the relay server and the home network server; and

using the secure channel, negotiating security parameters to establish the security association between the relay server and the home network server, wherein the security parameters comprise an encryption method, an integrity method, and a lifetime of the security association.

27. (New) The method of claim 21, wherein the tunnel between the home network server and the relay is an encrypted tunnel.

28. (New) The method of claim 21, wherein the tunnel between the home network server and the client is an encrypted tunnel.

29. (New) A method of establishing and maintaining secure communications between a home network server that is associated with a home network and a client when the client roams from the home network to a new location outside of the home network, the method comprising:

at the client, establishing a new Internet Protocol address associated with the new location, wherein the client has a permanent Internet Protocol address associated with the home network;

at the client, transmitting a registration message to the home server, wherein the registration message identifies the new Internet Protocol address associated with the permanent Internet Protocol address;

at the home network server, authenticating the registration message;

at the home network server, registering the new Internet Protocol address as a care-of-address for the client;

at the home network server, transmitting a reply message to the client confirming registration of the new Internet Protocol address as the care-of address for the client, thereby establishing a tunnel between the home network server and the client;

establishing a security association between the home network server and the client via the tunnel;

at the home network server, encapsulating the packets that are addressed to the client based on the security association between the home network server and the client;

for outbound traffic to the client, at the home network server, encapsulating the packets addressed to the client;

tunneling the encapsulated packets to the client, based on the security association between the home network server and the client, and the client's new Internet Protocol address;

at the client, decapsulating the encapsulated packets;

for inbound traffic to the home network server, at the client, encapsulating the packets addressed to the home network server;

tunneling the encapsulated packets to the home network server, based on the security association between the client and the home network server; and

at the home network server, decapsulating the encapsulated packets.

30. (New) The method of claim 29, wherein the home network comprises a firewall proxy.

31. (New) The method of claim 29, wherein establishing the security association between the home network server and the client comprises:

at the client, authenticating the home network server;

at the home network server, authenticating the client;

establishing a secure channel for negotiations between the client and the home network server; and

using the secure channel, negotiating security parameters to establish the security association between the client and the home network server, wherein the security parameters comprise an encryption method, an integrity method, and a lifetime of the security association.

32. (New) A method of establishing and maintaining secure communications between a home network server that is associated with a home network and a client

when the client roams from the home network to a new location outside of the home network, the method comprising:

at the client, establishing a new Internet Protocol address associated with the new location, wherein the client has a permanent Internet Protocol address associated with the home network, and the home network comprises a firewall;

at the client, transmitting a registration message in HTTP Request-Format to a relay server that is coupled to each of the client and the home network server, wherein the registration message identifies the new Internet Protocol address, and the relay server is located on a public side of the firewall;

at the relay server, authenticating the registration message;

at the relay server, encapsulating the registration message in at least one first user datagram protocol packet;

establishing a security association between the home network server and the relay server;

at the relay server, transmitting the at least one first user datagram protocol packet through the firewall to the home network server;

at the home network server, registering the new Internet Protocol address as a care-of-address for the client;

at the home network server, generating a reply message and encapsulating the reply message in at least one second user datagram protocol packet, wherein the reply message confirms registration of the new Internet Protocol address as the care-of address for the client;

at the home network server, transmitting the at least one second user datagram protocol packet to the relay server;

at the relay server, translating the at least one second user datagram protocol packet into HTTP Response-Format to generate a translated reply message;

at the relay server, upon a request from the client, transmitting the translated reply message to the client;

at the home network server, performing network address translation between the permanent Internet Protocol address and the new Internet Protocol address for packets addressed to the client;

at the home network server, encapsulating the packets that are addressed to the client;

at the home network server, tunneling the encapsulated packets to the relay server based on the security association between the home network server and the relay server, and the network address translation between the permanent Internet Protocol address and the new Internet Protocol address;

at the relay server, decapsulating the encapsulated packets; and

at the relay server, transmitting the decapsulated packets to the client.

33. (New) The method of claim 32, wherein establishing the security association between the home network server and the relay server comprises:

at the relay server, authenticating the home network server;

at the home network server, authenticating the relay server;

establishing a secure channel for negotiations between the relay server and the home network server; and

using the secure channel, negotiating security parameters to establish the security association between the relay server and the home network server, wherein the security parameters comprise an encryption method, an integrity method, and a lifetime of the security association.

34. (New) The method of claim 32, wherein establishing the security association between the home network server and the client comprises:

at the client, authenticating the home network server;

at the home network server, authenticating the client;

establishing a secure channel for negotiations between the client and the home network server; and

using the secure channel, negotiating security parameters to establish the security association between the client and the home network server, wherein the security parameters comprise an encryption method, an integrity method, and a lifetime of the security association.

35. (New) The method of claim 32, wherein the tunnel between the home network and the client is an encrypted tunnel.

36. (New) A method of establishing and maintaining secure communications between a home network server that is associated with a home network and a client

when the client roams from the home network to a new location outside of the home network, comprising:

at the client, establishing a new Internet Protocol address associated with the new location, wherein the client has a permanent Internet Protocol address associated with the home network, and the home network comprises a firewall and a multiplexer system;

at the client, transmitting a registration message in HTTP Request-Format to the firewall, wherein the registration message identifies the new Internet Protocol address;

at the firewall, authenticating the registration message;

at the firewall, transmitting the registration message to the multiplexer system;

at the multiplexer system, encapsulating the registration message in at least one first user datagram protocol packet;

at the multiplexer system, transmitting the at least one first user datagram protocol packet to the home network server;

at the home network server, registering the new Internet Protocol address as a care-of-address for the client;

at the home network server, generating a reply message and encapsulating the reply message in at least one second user datagram protocol packet, wherein the reply message confirms registration of the new Internet Protocol address as the care-of address for the client;

at the home network server, transmitting the at least one second user datagram protocol packet to the multiplexer system;

at the multiplexer system, translating the at least one second user datagram protocol packet into HTTP Response-Format to generate a translated reply message;

at the multiplexer system, transmitting the translated reply message to the client;

establishing a security association between the home network server and the client;

establishing an encrypted tunnel between the home network server and the client;

at the home network server, performing network address translation between the permanent IP address and the new Internet Protocol address for packets addressed to the client;

at the home network server, encapsulating the packets that are addressed to the client;

at the home network server, tunneling the encapsulated packets to the client based on each of the security association between the home network server and the client and the network address translation between the permanent Internet Protocol address and the new Internet Protocol address; and

at the client, decapsulating the encapsulated packets.

37. (New) The method of claim 36, further comprising:

for further outbound traffic to the client, at the home network server, encapsulating the packets addressed to the client;

tunneling the encapsulated packets to the client via the multiplexer system, based on the security association between the home network server and the client; and

at the client, decapsulating the encapsulated packets; and

for further inbound traffic to the home network server, at the client, encapsulating the packets addressed to the home network server;

tunneling the encapsulated packets to the home network server via the multiplexer, based on the security association between the client and the home network server; and

at the home network server, decapsulating the encapsulated packets.

38. (New) The method of claim 36, wherein establishing the security association between the home network server and the client comprises:

at the client, authenticating the home network server;

at the home network server, authenticating the client;

establishing a secure channel for negotiations between the client and the home network server; and

using the secure channel, negotiating security parameters to establish the security association between the client and the home network server, wherein the security parameters comprise an encryption method, an integrity method, and a lifetime of the security association.

39. (New) The method of claim 36, wherein the tunnel between the home network and the client is an encrypted tunnel.